Міністерство освіти і науки України

Національний Технічний Університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Студент групи ФБ-84

Киричук Тарас

Студент групи ФБ-84

Чипчев Дмитро

Перевірив:

Чорний О.М.

Київ - 2020

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата. 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи та опис труднощів

Спочатку було створено шифротекст(варіант 11) , пробіли букву "ё" замінили буквою "е" , а букву "ъ" буквою "ь" .Далі ми знайшли п'ять найчастіших біграм шифротексту . Далі ми реалізували розширений алгорим Еквліда, за допомогою якого можна знайти обернений елемнт за модулем, що необхідно для розв'язання лінійних порівнянь, та було розглянуто 3 випадки розв'язання. За допомогою формлул було знайдено пари ключів (a,b), які ще потрібно відсотрувати……

П’ять найчастіших біграм шифротексту:

1. “нк”
2. “юж”
3. “хб”
4. “шь”
5. “мк”

Зашифрований текст(варіант 11)

оквкпкящсройюфчвфбчллфэйлзщоыифуххгьижфбчбжройэжиавкхбоаэлбзьздблфюжвпыхожеуфыхьфисццоисцци
кшхгтчьюбрйэунемкщхлфэсццикоэйсыфляьэсблавххуоаебвщвцззабюжэйзэсюфцхцчьдвкьбивцкьхбвхщзфийамсьэ
хьжофшнйсбгежоэзхбннкндхбххьюэкублфйлщзхкгсебэуяффдзэсццоьзкжвхыфиамсьэтцщугтбйрипйпьуфптшью
уйукьлкуеафтбгфмсмешзчеюцнэпфиздббюакличуьлчяюеьххущьафюешзхксищфнлазьзьфююшлйапзгзхбфйсбцрп
тозкендзэнлбкнкщуюжбйдрптцьдьжьяжчэщлакэзйфбюыхожобьэгройюфеыхцылеимкжфлйутдяйиакютэффцйабгн
йакбхеыкжцлнььфьюдфбгьишллаяфеяфзьзжцазпзфижжнлмккцниулбргзхбтшяюйцуфьюпзмкабвхщугтбйлзтцсуяа
зяфыюедяьамсчежоакютэффцшжчядбоапздлчьпдкьуавкййлцыхяфнлвцаинарйлзщомксйуккзхьлзтцсуяамсчеылууе
зкзозуффыоайнтббйцилбвзщьцупзоулцафэйакюсзкшавкафэйоендхкыхзннложшушьмйыжбйоеахуиюиазезждрлрй
озвфьюяжсблзтцсубйчэбйфувккьбиыжмхбыотмхфыхцылкцбьмуксяфэлойэлтапзсфбззфйузядзозцьндкьдядзюцнэп
физчбющнкщугтбйяфюбфбшуэлтбыхожлфюжйсизсбрйэуэлсымсчеббвкслаклийияффшлаэлкцзьлсйуяфжнбкдбьэз
ээипуэлойчьшзкфяфицнкяилклзтцсуожоымехцэжшубкмьцфэйхьазцодбжройэщщройвмехщльзйжчячбэлрйычицхь
хихкрырйюжкжтуэлтбицщзщубгыфхцщбщьзцрипймкжфлйикххзцьхэлнктцчфлцждефэйоемазялвбйццакжтшьдфш
улэсбоеббвквещьэкеьюфукззщонихбмсйснгчьфшйсжртджапбляэфббозэиылшжохюжебиисйпчфзикозывмсойыцж
дяуяьрипйшкпзхбвхшлюгеыбйщуэлойактфнльжвхшьткхбшушьщыэфйуяфочшьцьдьсиртмкауэлойуиазезхкрилснг
ьлюджтнйыфьюшкябпфщжэлохщлыфизббвкейукыцйяпфлхмсоймкяждзацаьщьюцсйюжбкьэксюечбшуйудзфисцц
омкгзбкжинкчавктккхуилкххкнкуийиаьжнсдмуфпсамсьхоыозбицьохзнтбшьвфьлшзчебкфичбяфламсьхоыыжбйяфз
ннкозьхэлойэлвжшьсьхкчьчьскшьюкщэшьнджодбчясгэфнлсьхбсетцгьпйуклкцзнкшьюкщэшьуяфшебблшжчьтяпф
зийияфэсрйсфебгрчлчяфыяфэлтбвжчьтяпфукжфнезфжпфжвхюкщугтбйяфшлкцокшьюкщэшьнджоахакдйукмкхбо
жойшьазилеьпрпффцехпфцзткмущьщуыжхеылхккььомажрпзэжюкейэфзкэтеымехцэжнкчуюжьюсйюжххшбжсюй
гфнлмкактфожщлнйожткхбеххзьзкзткшлдяазмзбишлицхьсбоемкфждзацшлзилзыхгтуябкоквкпкйцпаюгбкйишьщз
пзхббйххптебькткширтйутдньвйгтяавкниеььяозшльщнкфшвхгтмкбькцрлеьгзттлвхкффэйсйюжххцтйуйувздбфыпз
визсрйцзычнйьюсьыэхьжомкчьюдьхксуяфзиоуфукфжсбщулэтбрйэумсьийиозэррйегдяозфиззикозшьюкюдчбьэыф
йсюжрйгфпфщлмкактфпфьжщлнйьиозщжэлнкаыйсюжрйгфарчжжппуехюжиьщжэлнкаыдяньлзычжспфщлсьхбсд
щлеьхиуиакнктдицщзкабйыжлзулфжэлчьцьньйишьхцпфнлззлбфыйннказезньпьтжксягэуйушжщлнйэлшзвлэуфых
ьщупзсцдбсхйуюжэфэйукьфеяебнйгфоафымелзюфлэыфцийидксыоавкчлфихкроюдьхожбйэфчязэнисдеьактфххмс
фиакюспфзнсыяфщлыдсйпблкцзэроблячжяхазслеижщнкикцьаклсюжпфбкикохбыыццзчкшлдящуехнеткшлыфчэб
йвпроцьохзнбйбйэфюенкозьхшвьэеуьзкзчксйюжххдяэфсыюжехгжцллфсепдщйукюдазцоозпащьгикьюгтайндяйлв
хшчицьзуехбхнтбознкооакжфдябкэфйнщпозеьлкцзиоюдпавклижочбфбйудзлхйуюбющнкзффзхфптэсожсюткьхэл
южщлжоцзеьуинйссыжезеяшьюкзфебэуйуйлыхдзсягхчьюбшуйуезхьчьзщнкцьтцгьсбоееьакюидьхьсбхбщьщзчиы
жчидунйдрттэсьвозулйафбзяхннкдяьахипазнойоаяфпбэуйулфсыюжикыйдяйлфцждщьэкеьщбюгтаююпаксьгиищз
пзхбпфбллкыхсбгфчяыфпбйуеятыньцьяисцыбюжщзйжьющьжжксягфйэфяьпмгьижмхбыцьшзыйяафбщфэйпфэлзя
ткфсзвткэрйсяьшлсбчжэфюжебяфххкьхцньежвхшцтцокфуфклбшсяаюжбйойодслсьхбизкннлжосыехщлхфюжэлщ

йцухцньяфьиьтощнкиккннлжовяцлнкэкрлчкхислшжщзйжьющььтяарйикхьыжщзйжьющььтэскьшчебфйсбшьзээф
сцтцвцикоошжшзхбьвгзфьакюсэсбящьюлкеыллйукыцйяпфыццзьлгзхавкхбкйцхьвфбмеэыывкьпущннйюжхунлис
ьвбказфидялзщоцьжфдящжтттцызеьуишзоочьщбфцщуеясббйньлзпзкьлкхкнкюыткфсгхюювгэфзкфжвхпумаехбюг
зоьпмгьшььвкьюдкьхкфбсьщфвзфкзлуиеьылйалцйиыьтжезюсцрщлмкактфьюшлсыхьшьззфцяфотмхеыыжбйфкэк
щьникьылнтнлждзьрылзнкисбйхужнююнкиячвьхьлкцгикьылууцьфькьбссбткдьхьлгьыхыжбйоечбюжмтчжфзвцл
зьзяцждяукжжнвхчяфкшамспьэикьылуудцуфбюакгапфиишьазщьцсицакикфисццортчкезлзрлкцзьчуйухбххцуыжп
азяэфжпеавкййдзтбрйфцщбьэртфимахичьясзяоттдазазезооскэимйлйоенквффыыфвхбйакнктдсжкстбчбфбдясдьжщ
ьцзщувзлиждщьэывкейыфдичбдзикхбщььзыискчьцьньроьхожойгфбюмкюквкхзюклккябехцзхбткькьнашупфьжок
сихкгежошлткиыххлэюснйчэбйеявхфжюзэфхбццшзябдиозмснгьжгзйфдзлзпзткнкюсфзиклирптзнйпчюжбклощхщ
нозхкмаобюерортнджоикпзтоозшсщнфкзльэщлнкззфидящьвггдхикьйиакхкбиинннлбияждзьясгэфцлхкьфющнкндй
иэигдкевкхбсдлавкбиьфцуэфйуяфочакябсхбясгэфшфщнбйыжяхьлюжчжебблеиззпзфсщлпбрсозюибкззасвкбьфбй
леьхкхбиипяьэлзйфьюмккцшзабгдкклыряймсебйубюгдчкшгяюмайнвхозэгяюнквфюжозикшсххойчярйфилйукыцйя
пфпафбтуюеромклхнйисзялзбиюлехойьлоифыкцгиьзообкохзнбйксццрфэсццаьбкьхыжксукичебфбсьмцлкчуйичьп
ршснкьхжройсхйнсдэннлыжакуфебкжбгньпьгьиявхжогьгишькннлжопыфбюжяавкэхманйгзоьпмгъьйукыцйяпфмк
гцлзюфяапбшьшчебзмлфнкшлчьцьньсыьэыфзкхццзежыфйснйэфвхгтиккьхикьыълэлткеякссбляфкфипьяиозяжнеия
фбхиьзяфксвхббоесыьэыфебьэщлчяпфщлткчллкыхтбукшьмкнкыльзньшьлзоежонцябюжьзщзьоююмкшьюкуеулщ
фюжюзжйебсехьакозвфзясгэфеыфбюжяьхббйеяцлсьхбйиазхункщулэсбгзжрвкроюдгьхбвхтбвщбисьидьфшвозмйп
тсбфимсшьфцфцсущннйюжхулфларйьэыфэлюжебблшжеьуийснйеыэлмктцэкэцдбяфожвхбкозмкбхйстбожфбгзоь
пмгьхцмсэфбхйсэфцуйубюмкоопдщлйиеьпршссбьхмсрйбьжооефшчвфбгфйснймяюзикмкоквкфитжсыэлжрхбазй
фбюгьгиозбкдбшвсйюжгзоьпмгьхццзозсйьгбйяфлиуцейыфвзсллкыхнйчьифпфсыюжбйтбоемкнкхкзжфбеькгвцчь
мктцгьхкхццзгзбьшьмккцбквцьзикжрткхкщйебляьияфйлждзьубрйэушуйуюбфбфбхиясиавкохзнбйчбфбяфнлззюяс
гэфцлсьхбсешьмхбыдзббвкйскьщьщутдрыньцьяфкжкснйкбпчяфмавкбклийирощжтттцызнквфехгтбклжсбсдхучя
югуилхбгыфсдьжозмкхбшэеяйньлюдшххнююойсыяфэуттйеифкжоайлчьйирошьцзхбщфвпохьгбыххлэнлжрйуыже
зткпяьэсджаехмсбиокщоакьхшущьодкьйироткежехмаюжртыикьнтеымеодкьйирыххлэззфжвхзябйннягхуежйсьжй
нуиэфщлакооакацынэфмкшзчйойэфэсехьэнзмкнкуфвхюгтбнйгфоамсбгйимкцйшэзиэлеьбкжийиромкежягчеяигзоь
пмгьшахисйнгбйоемаяфлйчбюжгззбихжезруозацткежехикхкиясгэфцлсьхбсееьакдяьэбкндхкндйлждзьжогзхфеяж
фдяткшйхузвфичьактфдршсвжнйцупфгидбжркйехгтбкикхкчкчэзэбьщоьжцлшудзэфртаксбехюжбксбоапзтджихбд
зчьцьхкроеьтжщпулахдзлкцхзясдптрйфбьлюдлаззждазйинибкрлсьсуцихбшедьщбщугтйнсдгрфпхьпьгьазйичьлгы
цюкмйсбткпзйфзясхждззулгрламсбкпащлыффцйидклфбзнквфехттюжюекцшькарйбккцфиьжфбткнкшьозжрпбшьу
уйугзнкмкхаждазпуежвхвяьлмкактффымеозфжмстккфыцждфьэшшвоечкфьифцрнйжртдидяябйннягхуьлйсфвхбхх
цуюжмкхббюьзчьцхзяакщугтбйгзнеазцоезикжфязтзозфуфпсьжясгэфйлыцылыцнамсчеуырйюжгкябьэщлнклйьфрт
кжмсткпзпьэйюдбзфуфпниубфэщлчямкиннлпфгтэсазгзжяозщьякцхсбизльдсюечкшлдяцьндмефшсбрйакуфлавкаф
эйоефкбкгежофбуихцылщфяамснгфцйишььхэфщлньдяятожыхйуфкхбпфюжойнлпцшушьвйзсшжфизфеыххлэмкс
йнгсюгзяфсывкнуэлчьцньяффзсйыщеьгьгишьыжьхожтцеьчьууйуюдикткхииолкцзэробькшьуябзыхьэебрссбююч
яьэсбяфяапзбхебтббленхичьафюжожддфбгцифшдяьэбкщщнкьясгэфщлюжезшзщлсьхбизсльхпбебблскулшзабьльхп
бебблшжфбюдщьэкеьюгблгрщфчэбйбзиоожакычхуяфдкьфэсехазиооемазяпзиочбненкюсцршсшснйебвжгзуцщщн
кэррйегбютшцуьлеьхцкннлзйыжбювзтзщулэеяозгзйннклфнльзщзьоцьэизфблчязффзиочьфцшьяжйссбоеюктжездо
ббщьйамсфигьсссбююактяфпшвцьрбщьакнумкхкжиозлзйенкиккьафцуфылццзозбискхбжпромсшьчкхбгхакккжфн
ликнкфубюэфэлуинбоаебшбьэыфэскифыехмсмкхкжоыжньфуйлкзаьжоьлвхгрвкмкнихбтбсещьжжчэбйвпропбрйэу
яфяазяэфжпьзкзчьзжйссбоешьесзягшуйухэыжббйуткнкфжсбляозчьзжездблцшзхбтбоербткмясгэфгкшьйлыхдзшь
чкшлдяэфщнукззщобьоозфщнтбуфыфхуфыхьсцлзгслэлаэллкыхсбэуйуяфыцхбвкыфбйэфяасчнйюжбйфзикушхуци
гдййьбузяшьюдзкьйчэбймахиапвикьыллшжсбвхафртшсяфэлойцпхьцьдьяясгэфдибьпзсдрусгеьбкеннкьхмсжпулскз
щодфыцйиыьжаххшэйуфбехфыцкйфцуфыхьозжилзжячэтццьтквкцзйфбяьлжрйучяиигьоонисучяэфьжксеяаквавкщ
урйцтхцньаксуьицьацыйтубйыцежвхююаьщьбььиьтеыххлэнлждзьылыгехьвафчэбккзхкваыфбявхбкйсфвпфизьхдр
нешсбйхушвхьгзуиюрвхсыюжцьрбщьыдьлэдеьдягьгихцтцгьпйукыцйяпфшльжшзхбукшавкафэйоемкфсбкбктоонн
кнксыехгтсцсихкхьгзакисццикмузяшььзюбфбоаньчьылыцэщнкюдэзффэйгзоьпмгьижкйптюертохюжебиимкэзчуи
дхцгьоониюыехэуехжсбйббифкжгирокамснгфцозхфсбшлиймачжбйяфшлхуяфззбкакуныфэлыцубгрлахиафойэлнн
нкфисццохбщьчфдзщьюлчьэиуфщлшфшубкгьоониюбрйэуттбйыжбйоесйптчяиивцулксжцозикшьохюжебойукыцй
япфпьуфптшьйайндякжоымехцэжшубкежвхтыххлэцркйгхнлдьцфббшфнльзвояфмкоцшлфжюжбйчьзжрйэлецозик
шлеьйиодэкнуфыхьпьэйбиокщоакшлиймачжюешьакозатцркйоекзпашубюсдслбклкьзклбцхбойоемкгзхбфисзмкюк
эзчуаьщьюцртебьиисфвпфвзэлнквксфюжобщфэйццфцяь